Pak. j. life soc. Sci. (2025), 23(1): 5333-5344 E-ISSN: 2221-7630;P-ISSN: 1727-4915

Pakistan Journal of Life and Social Sciences
www.pjlss.edu.pk

https://doi.org/10.57239/PJLSS-2025-23.1.00416

RESEARCH ARTICLE

The Impact of Digital Transformation on the Performance and Security of Information Systems in Government Institutions

Hondor Saragih

Defense University of the Republic of Indonesia

ARTICLE INFO

Received: Oct 29, 2024
Accepted: Jan 17, 2025

Keywords
Digital Transformation
Information Systems
Performance
Information Systems Security
Government Agencies
Cybersecurity

***Corresponding Author:**

hondor.saragih@idu.ac.id

ABSTRACT

Digital transformation has a significant impact on the performance and security of information systems in government agencies, which are increasingly dependent on technology to improve the efficiency and effectiveness of public services. In this context, the study adopts a mixed methods approach to explore and analyze the influence of digital transformation on two main aspects: information system performance and cybersecurity. The quantitative method was applied through a survey to 150 employees from five government agencies that have implemented digitalization, focusing on measuring performance such as the speed, accuracy, and productivity of information systems. A qualitative method was used to dig into in-depth perspectives through interviews with 20 decision-makers and IT staff regarding the challenges associated with security threats and risks that arise post-adoption of digital technologies. The results show that digital transformation improves the performance of information systems, reflected in operational efficiency and simplification of administrative procedures. However, the introduction of new technologies also introduces its vulnerability to cyberattacks, with an increase in threats both external and internal. These findings underscore the need for stronger security policies and risk mitigation strategies to support the long-term success of digital transformation in government agencies.

INTRODUCTION

In today's digital era, almost all sectors of life, including the public sector, are not immune to the influence of digital transformation (Millard, 2023). One of the most affected aspects is the application of information and communication technology (ICT) which has significantly changed the way government institutions carry out their duties and functions. Governments in various countries, including Indonesia, continue to strive to accelerate digital transformation in public institutions, with the aim of improving efficiency, transparency, accountability, and service to the community. The adoption of digital technology in the government sector is expected to reduce the burden on bureaucracy, speed up the administrative process, and increase interaction between the government and the community (Brunetti et al., 2020; Kumar et al., 2024; Rohayati et al., 2022).

However, while digital transformation provides many advantages in terms of information system performance, it also brings challenges that cannot be ignored, especially when it comes to cybersecurity (Wang et al., 2024). The deployment of more complex and globally connected digital systems increases the potential risk of cyber threats, such as hacking attacks, data leaks, and system disruptions that can damage the integrity of data and public services. Information system security in government institutions is a crucial aspect that needs to be carefully considered, because data managed by the government is often sensitive and vital for national and individual interests (Ahmad et al., 2022; Spears & Barki, 2010).

Digital transformation in government agencies includes various aspects of technology, such as the application of cloud computing, big data, Internet of Things (IoT), and artificial intelligence (AI) to improve the efficiency of data management and business processes (Spears & Barki, 2010). With this technology, government agencies can manage huge volumes of data faster and more accurately, reduce the potential for human error, and improve coordination between agencies. On the other hand, although this technology offers ease and improved quality of public services, many institutions are not fully prepared to face the challenges that come along with the adoption of this new technology. One of the big challenges is how to ensure that the

information systems implemented remain safe from cyber threats that continue to evolve (Shim et al., 2020; Thomas & Sule, 2023; Safitra et al., 2023).

Along with the digital changes that occur, the biggest challenge faced is cybersecurity. The government as a state administrator has a great responsibility in protecting citizens' personal data and sensitive data related to public policies, which if it falls into the wrong hands can have a very detrimental impact (Piduru, 2023). Data leakage incidents that have occurred in several countries show that weak security systems can undermine public trust in the government. Therefore, in addition to improving operational performance through digitalization, government agencies need to ensure that the systems they implement are equipped with adequate security policies and infrastructure (Hakim & Hayat, 2024; Hendrawan et al., 2024).

In general, digital transformation aims to improve the performance of information systems in government institutions, which is reflected in increasing time efficiency, data accuracy, and productivity in the implementation of administrative tasks (Yuniarti et al., 2024). The performance of this information system is highly dependent on how well digital technology is applied and integrated into existing processes. Therefore, it is very important to understand how the implementation of digital transformation affects the performance of government institutions, both in the day-to-day operational aspects and in efforts to achieve the strategic goals of the institution (Weber-Lewerenz, 2021; Vial, 2021; Burton-Jones et al., 2020).

However, the implementation of new technologies also introduces risks related to the security of information systems, which are often underestimated or even overlooked in the digital transformation process (Ismail et al., 2017). In many cases, weaknesses in existing security systems lead to increased potential for attacks from external parties, such as hackers or malware, as well as threats from inside, such as data leaks by employees. Neglected information system security can reduce the performance of government agencies, and can even cause large financial losses and damage the reputation of the institution. Therefore, there is a need for a well-integrated security strategy in every stage of digital transformation to ensure that the success of digitalization is not accompanied by losses caused by its vulnerabilities (Salem, 2016; Zhu et al., 2021; Mahraz et al., 2019).

Information System Security in Government Institutions is a very crucial aspect in today's digital era, considering that data and information managed by the government are very sensitive and have a wide impact on the country and its citizens. Government agencies manage a variety of important information, ranging from citizens' personal data, financial reports, public policies, to information related to national security. Therefore, the protection of this data and information system is not only important to maintain the integrity and confidentiality of information, but also to ensure that public services continue to run smoothly without interruption. Without adequate security systems, threats such as hacking, data leaks, and operational disruptions can undermine stability and public trust in the government.

The implementation of cybersecurity in government institutions must pay attention to various vulnerable points in the digital infrastructure used. Information systems connected to global networks are at greater risk of external attacks, such as hacking or malware. In addition, threats can also come from within the institution, such as data leaks by employees or abuse of system access by unauthorized parties. Therefore, it is important for government agencies to not only rely on software and firewalls to protect data, but also to ensure that internal policies and procedures related to access management and security training for employees are properly implemented. Strict access control systems, intensive monitoring, and regular audits of the use of information systems can help minimize the risks that arise.

However, despite the various security systems and policies that have been implemented, the biggest challenge in information system security in government agencies is the adoption of new technologies that often bring with them their own vulnerabilities. Digital transformation, such as the use of cloud computing, big data, and artificial intelligence (AI), does bring great advantages in improving data efficiency and accuracy. However, these new technologies also open up opportunities for more sophisticated and higher-risk cyberattacks. Complex system security requires more integrated and sustainable policies, as well as the readiness of government agencies to deal with evolving threats (Safitra et al., 2023). Therefore, strengthening cybersecurity is not only limited to the application of technology, but also includes long-term planning and cooperation between institutions to share information about existing cyber threats. That way, government agencies can be more prepared and responsive in the face of possible attacks

The purpose of this study is to investigate the impact of digital transformation on information system performance and information system security in government agencies, with a focus on institutions that have implemented digital technology in their operational activities. This study adopts a mixed methods approach, which combines quantitative and qualitative methods. The quantitative approach is used to measure the performance of information systems based on indicators such as operational efficiency, data accuracy, and public service productivity, while the qualitative approach is used to gain a deeper understanding of the security challenges and risks faced by government agencies, as well as how they deal with these issues.

Through a mixed methods approach, which combines quantitative and qualitative analysis, this study aims to examine the impact of digital transformation on the performance of information systems in government institutions, with a focus on improving efficiency, accuracy, and productivity. This research also seeks to identify various challenges faced in managing information system security after digital transformation, as well as analyze their impact on the stability and integrity of existing systems. In addition, this research will explore the security policies and strategies that government agencies need to implement to protect their information systems from cyber threats, as well as to ensure the sustainability and success of digitalization in the future. By relying on empirical data, this research is expected to provide in-depth insights and practical recommendations for policymakers and decision-makers in the public sector. The main goal is to formulate a more effective strategy in managing digital transformation, which not only pays attention to the aspect of improving performance, but also prioritizes information system security so that the negative impact of cyber threats can be minimized, while ensuring that digitalization in government institutions can take place in a sustainable and safe manner.

LITERATURE REVIEW

Along with the development of digital technology, digital transformation in the public sector is increasingly being applied in various countries (Schou & Hjelholt, 2018). According to Porter & Heppelmann (2014), digitalization has a positive impact on improving the operational efficiency of institutions, but also opens up opportunities for the emergence of cyber threats that require serious attention in terms of risk management. In this context, many studies show that information security is one of the key elements in the success of digital transformation. Zaydi (2024) emphasized the importance of risk management in dealing with threats arising from rapid system changes and high interconnection.

In this regard, Force & Initiative (2013) state that the performance of information systems will largely depend on the extent to which government agencies can integrate digital technology with effective security systems. If digital transformation is not balanced with serious attention to security, then the potential losses due to cyberattacks or data leaks can tarnish the successes achieved in terms of efficiency and productivity. Therefore, this study seeks to answer these challenges by connecting these two important dimensions, namely information system performance and cybersecurity, to provide a clearer picture of the impact of digital transformation in government institutions (Imran et al., 2021).

METHODOLOGY

This study adopts a mixed methods approach to analyze the impact of digital transformation on the performance and security of information systems in government institutions. This approach was chosen because it can combine the strengths of both quantitative and qualitative methods in providing a more comprehensive and in-depth picture of the topic being researched (Ahmad & Pandey, 2024; Lee et al., 2020).

1. Quantitative Approach

A quantitative approach is used to obtain objective and measurable data related to the performance and security of information systems. Quantitative data was collected through surveys using questionnaires distributed to employees and users of information systems in several government institutions that have undergone a digital transformation process (Hamilton & Chervany, 1981).

The questionnaire is designed to measure two main aspects:

1. Information System Performance: This dimension measures how effective and efficient the

information system is after digital transformation, which includes aspects of speed, accuracy, and ease of access to information.

2. Information System Security: This dimension measures the level of reliability and protection of data that exists in an information system, including the security policies implemented, user training, and the implementation of data security systems such as encryption and firewalls.

Respondents to this survey consisted of 150 employees who were directly involved in the use and management of information systems in selected government institutions. The data obtained was analyzed using descriptive and inferential statistical techniques, such as regression analysis to identify the relationship between digital transformation and improved system performance and security.

2. Qualitative Approach

A qualitative approach is used to dig deeper into the impact of digital transformation, which may not be fully revealed through quantitative data. Qualitative data was obtained through in-depth interviews with 20 respondents consisting of IT leaders and staff in government institutions that have implemented digital transformation (Agustian et al., 2023).

This interview aims to understand their subjective experience in managing and interacting with information systems after digital transformation is carried out. Interview questions are focused on two main things:

1. Changes in Information Systems Performance: This interview explores perceived changes in operational efficiency and effectiveness, including the challenges and successes experienced during and after the digital transformation process.

2. Information Systems Security: In this section, the interview aims to explore how security and data protection policies are implemented, as well as the perception of risks and threats that arise post-digital transformation.

The results of the interviews were analyzed with a thematic analysis approach to identify emerging themes related to the influence of digital transformation on the performance and security of information systems.

3. Quantitative and Qualitative Data Integration

The quantitative and qualitative data obtained will be analyzed simultaneously to provide a more holistic understanding of the impact of digital transformation. The results of the quantitative survey will be used to measure the extent to which digital transformation affects the performance and security of information systems, while the qualitative interviews will provide more context regarding the dynamics and experiences underlying the quantitative results (Plekhanov et al., 2023).

The unification of the results of these two approaches will be carried out through a data triangulation technique, where the findings from quantitative and qualitative analyses will be compared and combined to provide stronger and valid conclusions.

4. Validity and Reliability

To ensure the validity and reliability of the data, this study uses several techniques, including:

1. Validity Test: For questionnaires, validity is tested using exploratory factor analysis (EFA), while for interviews, validity is carried out by confirming findings through discussion with experts and respondents.

2. Reliability Test: For the questionnaire, reliability is tested using Cronbach's Alpha coefficient, with a value above 0.7 considered reliable. Qualitative interviews will also be ensured for reliability by triangulation between researchers.

5. Population and Sample

The population in this study is government institutions in Indonesia that have undergone digital transformation in the management of their information systems. The selection of the sample was carried out purposively, by selecting institutions that have been proven to carry out significant digital transformation and have operational information systems. The number of samples in the quantitative survey was 150 respondents, while the qualitative interviews involved 20 key informants from various levels of positions in the institution.

RESULTS AND DISCUSSION

This research aims to identify the impact of digital transformation on the performance and security of information systems in government institutions. Using a mixed methods approach, the quantitative and qualitative data collected provide a more complete picture of the impact of digital transformation. The results of the analysis are divided into two main parts: first, about the impact of digital transformation on the performance of information systems, and second, about the impact on information system security.

1. The Impact of Digital Transformation on Information System Performance

1.1. Quantitative Data

The survey, which was conducted on 150 respondents from 10 government agencies that have implemented digital transformation, showed a significant improvement in the performance of information systems. The data obtained from this survey was analyzed using linear regression to test the relationship between digital transformation and information system performance. The results of regression analysis indicate that digital transformation has a very significant positive influence on the performance of information systems, with a $p <$ value of 0.01, which means that there is a strong relationship between the two variables.

Some of the performance indicators used in this study to measure the impact of digital transformation are system response time, data accuracy, and ease of access to information. Each of these indicators provides a more detailed picture of the effectiveness of the application of digital technology in information management in government institutions.

1.1.1. System Response Time

Before digital transformation, the response time of the system used by government agencies required an average of 8.3 seconds per transaction. This shows that information systems that existed before digital transformation tended to be slow in responding to requests or commands from users. In the context of government agencies, slow response times can hinder operational efficiency, especially in data-driven decision-making.

After the implementation of digital transformation, especially through the use of cloud-based computing and automation-based systems, the system response time decreased to 3.5 seconds per transaction. This translates to a 57% increase in efficiency in terms of system speed in responding to requests. This decrease in response time can be explained by the application of faster and distributed technology, which allows data and information to be processed faster and with less manual intervention. This time efficiency is very important to speed up workflows and improve public services based on digital information systems.

1.1.2. Data Accuracy

The accuracy of data managed by information systems has also experienced a significant increase after the implementation of digital transformation. Before the transformation, the accuracy level of data managed by information systems in government institutions only reached 82%, which means that there are a number of errors in data management that can affect decision-making and the quality of public services.

However, after digital transformation, especially with the implementation of cloud computing-based technology that offers real-time data integration and more advanced data analytics systems, the data accuracy rate has increased to 95%. This increase indicates the existence of better and more accurate data management, which is obtained through a more organized and automated system. The application of advanced analytics technology allows the input data to be more valid and in accordance with the required standards, which of course has a positive impact on the quality of data-based reports, policies, and services.

1.1.3. Ease of Access to Information

Ease of access to information is also one of the important aspects in assessing the performance of information systems. Prior to digital transformation, around 40% of respondents reported difficulties in accessing information in real-time, indicating limitations in the technology infrastructure used. Delays in obtaining accurate data and information can hinder rapid decision-making processes, which in the context of government agencies have the potential to interfere with responding to emergency situations or urgent policy changes.

However, after the implementation of digital transformation, the use of cloud-based systems and the improvement of the overall IT infrastructure, the difficulty rate of information access decreased to 15%. This improvement shows significant progress in terms of real-time accessibility of data and information. The technology implemented allows employees and related parties to access the necessary data and information more easily, anytime and from anywhere, without having to depend on a certain time and place. This easier access will certainly increase the effectiveness and efficiency of public services and accelerate the decision-making process based on up-to-date data.

Table 1. Information System Performance Indicators

Performance Indicators	Before Digital Transformation	After Digital Transformation	Increase (%)
System Response Time (seconds)	8,3	3,5	57%
Data Accuracy (%)	82	95	13%
Ease of Access to Information (%)	40	15	62,5%

1.2. Qualitative Data

In-depth interviews conducted with 20 respondents from various levels of positions in 10 government agencies showed significant changes in operational processes after the implementation of digital transformation. Respondents from various positions, ranging from information technology (IT) unit managers, data management staff, to administrative officials, provided a consistent view on the positive impact of digital transformation on the performance and operational efficiency of their institutions. Many of them report significant efficiency improvements, especially in terms of data processing, which is now faster and more accurate, as well as a reduction in human error that was common in previous manual systems.

An IT unit leader at one of the institutions stated:

"Before the implementation of cloud-based systems and automation, processes that required large and complex data processing, such as monthly or annual reports, took days, or even longer. However, after the implementation of digital technology, the same process can now be completed in just a matter of hours, sometimes even in less than an hour. The cloud system used allows us to access data in real-time and process it more efficiently, while automation helps reduce the time spent on manual verification and repetitive data entry. This certainly has a direct impact on improving the performance of our units, not only in terms of time, but also in accuracy and more effective resource management."

This statement illustrates how significant the impact of the application of digital technology is on operational efficiency. Previously, government agencies had to rely on manual processes that took a long time and were prone to human error. Now, with cloud computing and automation systems, the time needed to complete

administrative tasks and data processing has been drastically cut, allowing institutions to be more responsive in providing public services.

In addition, data management staff at several institutions reported a significant decrease in complaints related to data speed and accuracy. Before digital transformation, many staff complained of difficulties in accessing data spread across various systems and formats. The process of ensuring accurate and complete data often takes a long time, with many manual procedures to be carried out. After the implementation of digital technology, especially the use of cloud-based systems and better integration between applications, data management has become more structured and accessible.

A data management staff at another institution explained:

"Previously, we often faced problems with difficulties in accessing data spread across various divisions. The data processing process is also very time-consuming because of the many manual procedures that we have to follow. However, since the cloud-based system was implemented, I was able to access all the data I needed with just a few clicks. In addition, we also reduced many data entry errors because many parts have now been automated. The speed and accuracy of the data has increased dramatically, which allows us to provide faster and more accurate reports to superiors and related parties."

Other respondents, who work in the administration, also gave a similar view. They report that before digital transformation, their biggest challenges were slow processing of documents and data, as well as difficulties in collaboration between units. After the transformation, the collaboration process became easier thanks to the use of a cloud-based platform that allows the exchange of information and documents in real-time. This not only increases the speed of processing, but also ensures that the information received by each party is always up-to-date and accurate.

Overall, these in-depth interviews show that digital transformation in government agencies not only reduces the time it takes to complete administrative tasks, but also improves the quality and accuracy of the data managed. The use of advanced technologies such as cloud computing and automation has brought about major changes in the way institutions manage information, making operational processes more efficient, responsive, and accurate. The application of this technology also has a positive impact on reducing manual workload and increasing employee productivity, which in turn supports improved performance and better public services.

2. The Impact of Digital Transformation on Information System Security

2.1. Quantitative Data

The application of new technology in the digital transformation process in government institutions not only has a positive effect on the performance of information systems, but also has a significant impact on the security aspect of information systems. Based on a survey conducted on 150 respondents in 10 government agencies, around 70% of respondents reported that the information security policies implemented after digital transformation are much stricter and more effective. Strengthening this security policy includes increasing the layer of protection for sensitive data, implementing stricter security protocols, and increasing security awareness and training for employees.

2.1.1. Data Security

One of the most prominent aspects of information security evaluation is the reduction in data leakage incidents. Prior to digital transformation, around 32% of respondents reported data leakage incidents in the last two years. These data leaks are often caused by insecure manual procedures, lack of oversight of data access, and limitations in the protection technology used. These leak incidents include the leakage of employees' personal information, sensitive public data, and internal reports that should not be known to outsiders.

However, after the implementation of more advanced digital technologies, including cloud-based systems with stronger data encryption protocols, the rate of data leakage has decreased drastically. Only 8% of

respondents reported a data leak incident after digital transformation, which indicates a 75% decrease in the frequency of data leaks. This decline illustrates the effectiveness of implementing encryption-based security and role-based access control that limits who can access sensitive data. In addition, the cloud computing technology used allows data to be stored in a secure and distributed location, reducing the risk of data loss or damage due to system failure.

2.1.2. Protection against Cyberattacks

Digital transformation also brings significant changes in protection against cyberattacks. Prior to the implementation of new technologies, cyberattacks such as malware, phishing, and ransomware were often a threat to government agencies' information systems. Based on respondents' reports, 15 cyberattacks occur per year on each institution, disrupting performance and causing considerable losses in the form of downtime and repair costs. These attacks typically occur due to weaknesses in legacy defense systems, including less sophisticated firewalls and a lack of updates to security software.

After digital transformation and the implementation of more advanced security systems, including new-generation firewalls and end-to-end data encryption, the incidence of cyberattacks has decreased significantly. The frequency of cyberattacks drops to 3 times per year. This 80% decrease shows that the new defense system is better able to detect and ward off external threats, reducing its vulnerability to attack. More advanced firewalls and the implementation of additional security techniques such as intrusion detection systems (IDS) and intrusion prevention systems (IPS) have strengthened the defense layer against more sophisticated attacks.

2.1.3. Compliance with Security Regulations

Another aspect that shows the success of digital transformation is the increase in compliance with applicable data security regulations. Prior to the implementation of digital transformation, only 50% of institutions consistently complied with data security regulations in accordance with standards set by governments and international agencies. This compliance is often hampered by limitations in terms of software used, as well as a lack of understanding of evolving regulations.

However, after the implementation of digital transformation, the level of compliance with these regulations has increased significantly, with 90% of institutions now meeting or even exceeding the set standards. This is inseparable from changes in stricter security policies, such as the implementation of stricter access controls, real-time monitoring of user activity, and security audits that are carried out regularly. In addition, the implementation of cloud-based encryption and security technologies also plays an important role in ensuring that data stored and processed by government agencies is in accordance with applicable regulations, reducing potential violations of personal data protection and information security regulations.

Table 2. The Impact of Digital Transformation on Information System Security

Safety Indicators	Before Digital Transformation	After Digital Transformation	Change (%)
Data Leak Incident (%)	32	8	75% decrease
Cyber Attacks (per year)	15	3	80% decrease
Security Regulatory Compliance (%)	50	90	40% increase

2.2. Qualitative Data

Statements from several key informants indicate that government agencies that are faster adapting to digital transformation are experiencing significant improvements in terms of data protection and their information security systems. The IT unit leaders and information systems managers interviewed revealed that the steps taken to implement new technologies, such as data encryption, advanced firewalls, and intrusion detection systems, have substantially strengthened the security layer in their institutions.

An IT manager at one of the government agencies revealed:

"After the implementation of the data encryption system and the use of advanced firewalls, we feel safer in managing sensitive data. The encryption system implemented not only secures data in transit, but also when it is stored, reducing the risk of leakage or unauthorized access. In addition, with a new generation of firewalls, we have a stronger layer of protection against external threats. We also conduct regular training for employees to ensure that security policies are always adhered to, as well as conduct regular system audits to detect potential gaps that may exist."

This statement reflects the growing confidence of institutions implementing advanced technology, where they feel better protected from the threat of data leaks and increasingly complex cyberattacks. The encryption technology applied to sensitive data, both at rest and in transit, provides a critical layer of protection. Additionally, the implementation of advanced firewalls and other security protocols that are more responsive to external threats suggests that these institutions have invested in more robust and sophisticated security systems.

However, while this digital transformation brings many improvements, some respondents also noted the challenges and technical constraints associated with the integration of new systems with pre-existing IT infrastructure. Most government agencies have old systems that have been in use for many years, and integrating them with new technologies often requires a lot of time and resources. Some respondents reported problems in system compatibility, where new technologies implemented could not always connect seamlessly with older systems. This can lead to bottlenecks in the flow of data between different systems and require time-consuming repairs or updates.

An administrative official at another institution explained:

"While we feel significant benefits from implementing the new security system, we also face some challenges in integrating this technology with existing legacy systems. Some of the applications we use are not fully compatible with the new cloud-based platform, which causes some technical difficulties in data transfer between systems. We also need longer to train employees to adapt to this new technology."

Other technical challenges include the limited capacity of the existing infrastructure. Some institutions mention that while new technologies such as cloud computing and data encryption offer many advantages, the existing infrastructure is not always enough to support the processing of larger, more complex data. In some cases, institutions are forced to upgrade their IT infrastructure, which requires additional budget and time for implementation.
However, overall, the majority of respondents in this study stated that digital transformation brought significant improvements in the aspect of data security and information systems. One of the other IT managers added:
"We are seeing a clear improvement in data protection after digital transformation. While there were some technical constraints and challenges in terms of integration, we felt that the steps taken were much more effective in keeping our data safe compared to the legacy systems we used previously. We hope that these challenges can be overcome as time goes on and our infrastructure capacity strengthens."

Overall, despite the obstacles in the process of system integration and HR training, which is a common challenge in any major digital transformation project, the results achieved in improving data security and information systems are significant. Government agencies that are faster to adapt to new technologies feel much more secure in managing their sensitive data. The implementation of more sophisticated security systems and increasing the capacity of information technology infrastructure are expected to continue to strengthen resilience to external threats, as well as ensure that data managed by government agencies is well protected. Going forward, these institutions plan to continue to improve their technical capabilities and strengthen collaboration between IT units and other units in order to overcome the integration challenges that still exist.

3. Performance and Security Impact Integration

The unification of findings from quantitative and qualitative data in this study shows that the positive impact

of digital transformation on the performance and security of information systems in government institutions is not a stand-alone phenomenon, but two aspects that are interrelated and mutually reinforcing each other. The increase in the efficiency and speed of information systems recorded in quantitative data, such as a decrease in system response time, an increase in data accuracy, and ease of access to information, has a significant impact on the improvement of information system security revealed through interviews with key informants. More structured and well-managed data facilitates the implementation of more effective security policies, as faster and more efficient systems allow for better risk management and faster response to potential threats or attacks.

One of the key findings in quantitative data is a significant decrease in the incidence of data leaks and cyberattacks after the implementation of digital technologies, such as data encryption and advanced firewalls. Based on the survey results, data leaks decreased by 75%, while the incidence of cyberattacks decreased drastically by 80%. These findings are particularly relevant to qualitative data obtained from in-depth interviews, where many respondents reported that the application of digital technology not only improves operational efficiency, but also provides better protection against sensitive data. A more structured system makes it easier for agencies to monitor, control, and secure data from potential more complex threats.

Further, the IT managers and unit leaders interviewed explained that with the implementation of cloud-based systems and encryption technologies, they feel much safer in managing sensitive data. The use of encryption technology that applies not only to the data being transmitted but also to the data being stored reduces its vulnerability to unauthorized access or leaks caused by system failures. Cloud systems allow institutions to manage and store data in a more centralized and secure manner, while more sophisticated firewalls provide an additional layer of protection against cyberattacks from outside.

4. Performance and Security Convergence in Digital Transformation

One of the interesting aspects found in this analysis is the interdependent relationship between the performance and security of information systems. Operational efficiency achieved through the application of digital technology, such as increased data processing speed, reduction of human error, and ease of access to information, directly contributes to the strengthening of the security system. More structured and better managed data becomes easier to secure. For example, with a faster and more efficient system, agencies can identify and respond to potential threats or incidents of data leaks more quickly. The ability to monitor data flows and conduct audits in real-time allows for early detection of potential problems, which in turn strengthens resilience to external threats.

In particular, the results of qualitative interviews show that several institutions that have adopted digital technology first admitted that they feel better prepared to face cyber threats and other disturbances. One of the key informants who served as IT manager stated:

"We realize that the implementation of cloud technologies and automation not only increases the speed of our internal processes, but also strengthens the defense system against external threats. With well-managed and more structured data, it's easier for us to detect suspicious conversations or unauthorized access attempts. In addition, our speed in responding to security incidents is much better than before."

The results of these findings are very relevant to the Technology-Organization-Environment (TOE) theory, which explains that the adoption of technology in organizations, especially those related to information technology infrastructure, can improve the operational performance and security of information systems at the same time. The TOE model states that three main factors—technology, organization, and the external environment—must support each other to ensure the success of digital transformation within an organization. In the context of this study, the application of new technologies in government agencies can improve operational efficiency while strengthening defense against cyber threats, as long as there is good support from within the organization (including human resources and security training) and effective integration between systems.

The implementation of digital technology in government agencies also shows the importance of management support and collaboration between the information technology unit and other units in the organization. For example, in some cases, the success of digital transformation depends not only on the application of the

technology itself, but also on the seamless integration between the new system and the existing infrastructure. Without good support in terms of coordination between units and adequate resources, efforts to improve performance and security can be hampered. Therefore, it is important for organizations to ensure that new technologies can go hand in hand with internal policies and compliance with external regulations.

5. Implications and Recommendations

Overall, these findings confirm that digital transformation in government agencies has a significant impact not only on improving operational performance, but also on strengthening information security systems. Successful transformation to create a more efficient and secure technology ecosystem relies heavily on effective integration between technology, organizations, and the external environment, in accordance with the TOE framework. Therefore, government agencies need to ensure that they are not only focused on implementing new technologies, but also pay attention to aspects of organizational support, including employee training, policy updates, and strengthening existing IT infrastructure.

To improve the results of this digital transformation, it is recommended that government agencies:

1. Improving system integration between old and new technologies to ensure smooth data flow and reduce potential operational disruptions.
2. Develop cybersecurity training for all employees to ensure that security policies can be properly complied with and preventive measures can be taken effectively.
3. Conduct periodic audits of the system to identify potential gaps or vulnerabilities, as well as update security systems according to technological threats.
4. Strengthen collaboration between units in government institutions so that each unit can support the implementation of technology effectively and sustainably.

Thus, digital transformation is not only about the adoption of new technologies, but also about creating a mutually supportive ecosystem, between technology, policy, and human resources, to achieve greater goals in terms of operational efficiency and data security.

CONCLUSION

Based on the results of the research, it can be concluded that digital transformation has a significant impact on the performance and security of information systems in government institutions. The improvement in information system performance is reflected in a significant decrease in response time, increased data accuracy, and ease of access to information. The use of cloud-based technology and automation of operational processes has proven to be effective in improving the efficiency and effectiveness of information management, which in turn has a direct impact on improving the performance of the institution. In addition, digital transformation also brings significant strengthening in the security aspect of information systems. The incidence of data leaks and cyberattacks has decreased drastically after the implementation of data encryption technology, more advanced firewalls, and stricter security policies. Furthermore, the level of compliance with data security regulations is increasing, indicating that the institutions studied are now better able to keep their information safe.

The findings of this study also reveal that the performance and security of information systems are interrelated. Increased system efficiency and accuracy allow for more structured data management, which indirectly strengthens the security aspect. A faster and more accurate system makes it easier to detect potential threats and minimize the risk of data leaks. While there are still challenges related to the integration of new technologies and the need for continuous training for human resources, overall, the benefits obtained from digital transformation far outweigh the existing constraints. Therefore, government agencies are expected to continue and deepen their digital transformation, with a focus on improving system integration and strengthening human resource capacity in managing information technology more securely and effectively. Thus, digital transformation in government institutions can not only improve the quality of information system management, but also support governance that is more efficient, transparent, and responsive to the needs of the community.

REFERENCES

Agustian, K., Mubarok, E. S., Zen, A., Wiwin, W., & Malik, A. J. (2023). The Impact of Digital Transformation on Business Models and Competitive Advantage. *Technology and Society Perspectives (TACIT)*, *1*(2), 79–93.

Ahmad, K., Maabreh, M., Ghaly, M., Khan, K., Qadir, J., & Al-Fuqaha, A. (2022). Developing future human-centered smart cities: Critical analysis of smart city security, Data management, and Ethical challenges. *Computer Science Review*, *43*, 100452.

Ahmad, K., & Pandey, N. (2024). A mixed methods study to uncover the adoption potential of digital marketing in Indian SMEs. *Asian Journal of Economics, Business and Accounting*, *24*(4), 168–181.

Brunetti, F., Matt, D. T., Bonfanti, A., De Longhi, A., Pedrini, G., & Orzes, G. (2020). Digital transformation challenges: strategies emerging from a multi-stakeholder approach. *The TQM Journal*, *32*(4), 697–724.

Burton-Jones, A., Akhlaghpour, S., Ayre, S., Barde, P., Staib, A., & Sullivan, C. (2020). Changing the conversation on evaluating digital transformation in healthcare: Insights from an institutional analysis. *Information and Organization*, *30*(1), 100255.

Force, J. T., & Initiative, T. (2013). Security and privacy controls for federal information systems and organizations. *NIST Special Publication*, *800*(53), 8–13.

Hakim, A., & Hayat, A. (2024). Transforming Public Policy in Developing Countries: A Comprehensive Review of Digital Implementation. *Journal of ICT Standardization*, *12*(3), 337–364.

Hamilton, S., & Chervany, N. L. (1981). Evaluating information system effectiveness-Part I: Comparing evaluation approaches. *MIS Quarterly*, 55–69.

Hendrawan, S. A., Chatra, A., Iman, N., Hidayatullah, S., & Suprayitno, D. (2024). Digital transformation in MSMEs: Challenges and opportunities in technology management. *Jurnal Informasi Dan Teknologi*, 141–149.

Imran, F., Shahzad, K., Butt, A., & Kantola, J. (2021). Digital transformation of industrial organizations: Toward an integrated framework. *Journal of Change Management*, *21*(4), 451–479.

Ismail, M. H., Khater, M., & Zaki, M. (2017). Digital business transformation and strategy: What do we know so far. *Cambridge Service Alliance*, *10*(1), 1–35.

Kumar, S., Verma, A. K., & Mirza, A. (2024). *Digital Transformation, Artificial Intelligence and Society*. Springer.

Lee, S.-H., Choi, S.-J., & Kim, H.-W. (2020). What makes people send gifts via social network services? A mixed methods approach. *Internet Research*, *30*(1), 315–334.

Mahraz, M.-I., Benabbou, L., & Berrado, A. (2019). A systematic literature review of digital transformation. *Proceedings of the International Conference on Industrial Engineering and Operations Management*, 917–931.

Millard, J. (2023). *Impact of digital transformation on public governance*. Joint Research Centre (Seville site).

Piduru, B. R. (2023). Cybersecurity And Customer-Centric Government Services: Protecting Citizen Data And Trust. *International Journal of Machine Learning and Cybernetics (IJMLC)*, *1*(1), 35–45.

Plekhanov, D., Franke, H., & Netland, T. H. (2023). Digital transformation: A review and research agenda. *European Management Journal*, *41*(6), 821–844.

Rohayati, Y., Bangkara, B. A., Fkun, E., Iskandar, A., & Jacob, J. (2022). Understanding the Roles and Challenges of Local Government in the Era of Technological Transformation in Indonesia: A Study of Public Policy Literacy. *ARISTO*, *10*(3), 566–590.

Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking cyber threats: A framework for the future of cybersecurity. *Sustainability*, *15*(18), 13369.

Salem, F. (2016). A Smart City for public value: Digital transformation through agile governance-the case of'Smart Dubai'. *World Government Summit Publications*.

Schou, J., & Hjelholt, M. (2018). *Digitalization and public sector transformations*. Springer.

Shim, J. P., Sharda, R., French, A. M., Syler, R. A., & Patten, K. P. (2020). The Internet of Things: Multi-faceted research perspectives. *Communications of the Association for Information Systems*, *46*(1), 21.

Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. *MIS Quarterly*, 503–522.

Thomas, G., & Sule, M.-J. (2023). A service lens on cybersecurity continuity and management for organizations' subsistence and growth. *Organizational Cybersecurity Journal: Practice, Process and People*, *3*(1), 18–40.

Vial, G. (2021). Understanding digital transformation: A review and a research agenda. *Managing Digital Transformation*, 13–66.

Wang, S., Asif, M., Shahzad, M. F., & Ashfaq, M. (2024). Data privacy and cybersecurity challenges in the digital transformation of the banking sector. *Computers & Security*, *147*, 104051.

Weber-Lewerenz, B. (2021). Corporate digital responsibility (CDR) in construction engineering—ethical guidelines for the application of digital transformation and artificial intelligence (AI) in user practice. *SN Applied Sciences*, *3*, 1–25.

Yuniarti, S., Hadmar, A. M., Zaenuri, M., & Mutiarin, D. (2024). Digital Transformation in Civil Service Management: Implementing the SmartASN Platform. *Society*, *12*(2), 381–396.

Zaydi, M. (2024). A new framework for agile cybersecurity risk management. *Agile Security in the Digital Era: Challenges and Cybersecurity Trends*, *19*.

Zhu, X., Ge, S., & Wang, N. (2021). Digital transformation: A systematic literature review. *Computers & Industrial Engineering*, *162*, 107774.